2011

Cyber Attacks as "Force" Under UN Charter Article 2(4)

Matthew C. Waxman
Columbia Law School, mwaxma@law.columbia.edu

III

Cyber Attacks as "Force" under UN Charter Article 2(4)

Matthew C. Waxman*

In a 2010 article in *Foreign Affairs*, Deputy Secretary of Defense William Lynn revealed that in 2008 the Department of Defense suffered "the most significant breach of U.S. military computers ever" when a flash drive inserted into a US military laptop surreptitiously introduced malicious software into US Central Command's classified and unclassified computer systems.[1] Lynn explains that the US government is developing defensive systems to protect military and civilian electronic infrastructure from intrusions and, potentially worse, disruptions and destruction, and it is developing its own cyber-strategy "to defend the United States in the digital age."[2]

To what extent is existing international law, including the UN Charter, adequate to regulate cyber attacks and related offensive and defensive activities today and in the future? By "cyber attacks" I mean efforts to alter, disrupt, degrade or destroy computer systems or networks or the information or programs on them.[3]

This article examines one slice of that legal puzzle: the UN Charter's prohibitions of the threat or use of "force" contained in Article 2(4).[4] Other writings in this volume deal with questions such as Article 51's self-defense provisions and questions of State responsibility, and there are other international legal prohibitions and regulations that are relevant as well. But Article 2(4) is a good place to start

* Associate Professor of Law, Columbia Law School.

because it establishes or reflects foundational principles upon which most international law regulating international security sits. As a general matter, military attacks are prohibited by Article 2(4) except in self-defense or when authorized by the UN Security Council. Also as a general matter, most economic and diplomatic assaults or pressure, even if they exact tremendous costs on a target State, are not barred in the same way. Where along the spectrum in between might cyber attacks—which have some attributes of military attacks and some attributes of non-military pressure—lie?

Almost a decade ago, in a previous volume of this series, Professor Yoram Dinstein observed of cyber attacks: "The novelty of a weapon—any weapon—always baffles statesmen and lawyers, many of whom are perplexed by technological innovation. . . . [A]fter a period of gestation, it usually dawns on belligerent parties that there is no insuperable difficulty in applying the general principles of international law to the novel weapon . . . ."[5] This article takes up that claim in examining how US officials, scholars and policy experts have sought to adapt the UN Charter's basic principles.

This analysis yields two descriptive insights. First, it shows that American thinking (both inside and outside the government) inclines toward reading prohibited "force" broadly enough to include some hostile actions that might be carried out with bits of data in cyberspace. Although not necessarily inconsistent with interpretations previously dominating American thinking, this recent inclination reflects a shift away from the stricter readings of Article 2(4) and related principles that the United States government defended in the past when it was often the United States and its allies resisting efforts by some other States to read "force" broadly or flexibly.

Second, any legal line drawing with respect to force and modes of conflict has distributive effects on power, and it is therefore likely to be shaped by power relations. Because States have different strategic cyber-capabilities and different vulnerabilities to those capabilities, it will be difficult to reach international consensus with regard to the UN Charter's application to this problem.

Article 2(4) and the Meaning of "Force"

Modern legal regulation of force and conflict begins with the UN Charter, and specifically Article 2(4), which mandates that "[a]ll Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations."[6] Article 51 then provides that "[n]othing in the present Charter shall impair the inherent right of individual or

collective self-defense if an armed attack occurs against a Member of the United Nations."[7] Although significant debate exists about the scope of self-defensive rights to resort to military force, it is generally agreed that the use of military force authorized under Article 51 is not prohibited under Article 2(4).[8]

With respect to offensive cyber-capabilities and the UN Charter, then, these provisions raise several major questions: In terms of Article 2(4), might a cyber attack constitute a prohibited "use of force"? If so, might a cyber attack give rise to a right to use military force in self-defensive response pursuant to the rights reserved in Article 51?[9] The latter question is taken up in more detail in another article in this volume, but because the two provisions operate in tandem it is important to bear in mind self-defense remedies here as well.

Global interconnectedness brought about through information technology gives States and non-State actors a powerful potential weapon. Military defense networks can be remotely disabled or degraded. Flooding an Internet site, server or router with data requests to overwhelm its capacity to function—so-called "denial of service" attacks—can be used to take down major information networks, as demonstrated by an attack on Estonia (a country especially reliant on Internet communications) during 2007 diplomatic tensions with Russia.[10] Private-sector networks can be infiltrated, damaged or destroyed.[11]

Some experts speculate that the United States is at particularly heightened risk because of its tremendous economic and military dependency on networked information technology.[12] As the Obama administration's 2010 National Security Strategy acknowledged,

> [t]he very technologies that empower us to lead and create also empower those who would disrupt and destroy. They enable our military superiority, and . . . [o]ur daily lives and public safety depend on power and electric grids, but potential adversaries could use cyber vulnerabilities to disrupt them on a massive scale.[13]

Such possibility that massive harm could be perpetrated in cyberspace, rather than physical space, raises questions whether the UN Charter's foundational prohibitions and authorities—which were drafted with conventional warfare in mind—apply or should apply to such conduct.

The dominant view in the United States and among its allies has long been that Article 2(4)'s prohibition of force and the complementary Article 51 right of self-defense apply to military attacks or armed violence.[14] The plain meaning of the text supports this view, as do other structural aspects of the UN Charter. For example, Articles 41 and 42 authorize, respectively, the Security Council to take actions not involving armed force and, only should those measures be inadequate, to escalate

to armed force. There are textual counterarguments, such as that Article 51's more specific limit to "armed attacks" suggests that drafters envisioned prohibited "force" as a broader category not limited to particular methods, but the discussions of means throughout the document suggests an intention to regulate armed force more strictly than other instruments of power, and this narrow interpretation has generally prevailed.

An alternative view of Article 2(4) looks not at the instrument used but its purpose and general effect: that it prohibits coercion. Kinetic military force is but one instrument of coercion, and often the easiest to observe. At various times some States—usually those of the developing world or, during the Cold War, the "Third World"—have pushed the notion that "force" includes other forms of pressure, such as political and economic coercion that threatens State autonomy.[15] During the Charter's early years, debates similar to that over Article 2(4)'s definition of "force" also played out in the UN General Assembly over how to define prohibited "aggression." The United States and its Western allies pushed a narrow definition of "aggression," focused on military attacks, while developing States advocated an expansive definition to include other forms of coercion or economic pressure.[16] A problem with the latter approach has always been the difficulty of drawing lines between unlawful coercion and lawful pressure, since coercion in a general sense is ever-present in international affairs and a part of everyday inter-State relations.[17]

A third possible approach toward interpreting Article 2(4) and related principles focuses on the violation and defense of rights; specifically, that it protects States' rights to freedom from interference. Such an approach might tie the concept of force to improper meddling or intrusion of the internal affairs of other States, rather than a narrow set of means. Again, during the Charter's early years it was often the Third World pushing this view, as expressed in UN General Assembly resolutions.[18] Aside from the weak textual support for this approach, pragmatic considerations precluded the much wider interpretation, though this approach brings to mind possible analogies of cyber attacks to other covert efforts to undermine political or economic systems, such as propaganda efforts.

To whatever extent Article 2(4)'s meaning was settled and stable by the end of the Cold War in favor of a narrow focus on military force, cyber warfare poses challenges and tests the Charter's bounds. Offensive cyber attack capabilities such as taking down government or private computer systems share some similarities with kinetic military force, economic coercion and subversion, yet also have unique characteristics and are evolving rapidly. The possibility of cyber attacks therefore raises difficult line-drawing questions and requires re-examination of previous US legal strategy toward Charter interpretation.

Emergent US Interpretation

The examples of competing interpretations drawn from early legal debates over the UN Charter are useful for two reasons. First, they help show that some fundamental issues involved in current discussions of cyber attacks are not entirely new or unique to cyber-technology. Modes and technologies of conflict change, and the law adjusts with varying degrees of success to deal with them. Second, they highlight some subtle but important realignments of US legal-strategic interests.

The United States government has not articulated publicly a general position on cyber attacks and Articles 2(4) and 51, though no doubt internally the US government's actions are guided by extant legal determinations developed through interagency deliberation. There is, in the meantime, considerable momentum among American scholars and experts toward finding that some cyber attacks ought to fall within Article 2(4)'s prohibition on "force" or could constitute an "armed attack," insofar as those terms should be interpreted to cover attacks with features and consequences closely resembling conventional military attacks or kinetic force. The National Research Council convened a committee to study cyber warfare. It concluded that cyber attacks should be judged under the UN Charter and customary *jus ad bellum* principles by considering whether the *effects* of cyber attacks are tantamount to a military attack.[19] Michael Schmitt, in a seminal article on the topic, proposes that whether a cyber attack constitutes force depends on multiple factors that characterize military attacks, including severity, immediacy, directness, invasiveness, measurability and presumptive legitimacy.[20] Other legal experts have proposed similar tests emphasizing effects,[21] and some policy experts have come to similar conclusions in terms of US defensive doctrine against cyber attacks. Richard Clarke, for example, proposes a doctrine of "*cyber equivalency*, in which cyber attacks are to be judged by their effects not their means. They would be judged as if they were kinetic attacks, and may be responded to by kinetic attacks, or other means."[22]

Statements by senior US government officials have either hinted that the United States would regard some cyber attacks as prohibited force or declined to rule out that possibility. In 1999, the Defense Department's Office of the General Counsel produced an *Assessment of International Legal Issues in Information Operations.* That report noted:

> If we focused on the means used, we might conclude that electronic signals imperceptible to human senses don't closely resemble bombs, bullets or troops. On the other hand, it seems likely that the international community will be more interested in the consequences of a computer network attack than its mechanism.[23]

It further suggested that cyber attacks could constitute armed attacks giving rise to the right of military self-defense.[24]

Recent statements by senior US government officials appear consistent with that view. In a 2010 address, Secretary of State Hillary Clinton declared US intentions to defend its cybersecurity in terms similar to those usually used to discuss military security:

> States, terrorists, and those who would act as their proxies must know that the United States will protect our networks. . . . Countries or individuals that engage in cyber attacks should face consequences and international condemnation. In an interconnected world, an attack on one nation's networks can be an attack on all.[25]

In testifying before the Senate committee considering his nomination to head the new Pentagon Cyber Command, Lieutenant General Keith Alexander explained that "[t]here is no international consensus on a precise definition of a use of force, in or out of cyberspace. Consequently, individual nations may assert different definitions, and may apply different thresholds for what constitutes a use of force."[26] He went on, however, to suggest that "[i]f the President determines a cyber event does meet the threshold of a use of force/armed attack, he may determine that the activity is of such scope, duration, or intensity that it warrants exercising our right to self-defense and/or the initiation of hostilities as an appropriate response."[27] Implicit here seems to be a notion that "force" is, to some extent, about effects or consequences of hostile actions.

The United States government probably prefers an effects-based or consequences-based interpretation of "force" or "armed attack" with respect to cyber attacks for what it prohibits, as well as for what it does not prohibit. Under such an approach, for example, computer-based espionage, intelligence collection or perhaps even preemptive cyber-operations to disable hostile systems would not constitute prohibited force, because they do not produce direct or indirect destructive consequences analogous to a military attack.[28] As former National Security Agency Director Michael Hayden recently remarked, "Without going into great detail, we're actually pretty good at [cyber-espionage]."[29] Hayden's comment helps illustrate also a reason why it will be difficult for the United States government to develop and articulate clear legal positions on what sorts of actions in cyberspace constitute illicit force: because the key agencies have divergent policy priorities amid a rapidly evolving strategic environment. Some agencies are charged with protecting the integrity of US military capabilities; some are dedicated to intelligence collection, often involving infiltration of foreign computer networks and information systems; some prioritize protecting US civilian infrastructure, including the private sector's;

and others are focused on transnational law enforcement and enhancing international cooperation. These divergent policy priorities probably make it difficult to agree on how broadly or narrowly to draw legal lines, whether to drive toward legal clarity at all, and whether to engage publicly or diplomatically on these points.

Challenges of Regulating Cyber-"Force"

Even if Article 2(4) is interpreted to prohibit some forms of offensive cyber attacks, it would prove difficult to apply and enforce that prohibition. The difficulties of regulating certain types of conflicts in earlier eras of UN history help demonstrate these challenges.

Lamenting in 1970 the "death" of Article 2(4), Professor Thomas Franck assessed that rapid changes in the way conflict was waged had made its prohibitions of force obsolete. Whereas "[t]he great wars of the past, up to the time of the San Francisco Conference, were generally initiated by organized incursions of large military formations of one state onto the territory of another, incursions usually preceded by mobilization and massing of troops and underscored by formal declarations of war," Franck observed that "[m]odern warfare . . . has inconveniently by-passed these Queensberry-like practices."[30] Superpowers routinely supported insurgencies, rebel movements and coups against States supporting the other power with various forms of assistance, including arms. Small-scale wars and subversion and counter-subversion waged through local proxies became a common mode of superpower conflict, rather than direct, conventional military action.[31] The UN Charter regime was ill equipped to handle conflict that unfolded in these ways.

Franck's concern was that modes of conflict had outstripped the UN Charter regime's ability to impose costs on purported violators. Indeed, whatever costs Article 2(4) imposed on conventional military attacks across borders may even have pushed antagonists toward other modes of conflict. In another volume of this series dedicated to what was often referred to as "low-intensity conflict," Alberto Coll remarked in 1995 that "[t]he high political, military, and economic risks increasingly associated through the course of the twentieth century with open, conventional war have led many States and non-State entities to shift to other forms of violence as instruments of foreign policy."[32] Robert Turner agreed, noting that "the low-intensity conflict scenario is selected because it provides a colorable claim of legitimacy (being less obvious)."[33]

Questions for conflict in cyberspace then follow: Can Article 2(4)'s constraints adjust to cyber-capabilities in ways that differentiate illicit conduct from legal, and in ways that help impose costs for non-compliance? Can such interpretations command the respect of powerful actors in the international system?

One reason why cyber attacks will be difficult to regulate is that the factual bases for asserting a violation of 2(4)—or a right of armed self-defense under Article 51—will be subject to great uncertainty and difficult to verify. Some technologies or modes of conflict pose special challenges for international legal regulation because their attributes match poorly with the enforcement mechanisms, which sometimes include formal processes like UN Security Council review but more often involve decentralized assessment and evaluation by individual States, international bodies and other influential international actors.[34]

Those who study the problem of legally regulating cyber attacks usually point to the tricky problem of attribution. That is, it will often be difficult to discern quickly and accurately who launched or directed an attack.[35] The nature of electronic informational infrastructure and the limits of forensic capabilities are such that it may be impossible technically to link an attack to the party ultimately responsible.[36] As Deputy Secretary Lynn put it, "It is difficult and time consuming to identify an attack's perpetrator. Whereas a missile comes with a return address, a computer virus generally does not. The forensic work necessary to identify an attacker may take months, if identification is possible at all."[37]

Again, though, this is not an entirely new problem for Article 2(4), because similar attribution issues arose in the context of Cold War proxy warfare and low-intensity conflict. "The small-scale and diffuse but significant and frequent new wars of insurgency have," explained Franck in 1970, "made clear-cut distinctions between aggression and self-defense, which are better adapted to conventional military warfare, exceedingly difficult."[38] Furthermore, "[w]ith the hit-and-run tactics of wars of national liberation, on the other hand, it is often difficult even to establish convincingly, from a pattern of isolated, gradually cumulative events, when or where the first round began, let alone at whose instigation, or who won it."[39] Unconventional warfare and support for insurgencies and counterinsurgencies often by design featured inconclusive evidence of foreign involvement or hostile action, and foreign State antagonists worked to mask, conceal or obscure their participation.[40] This legal-factual murkiness helps explain why Article 2(4) seemed so impotent in addressing that form of conflict and why that mode of conflict offered an appealing option to the Cold War antagonists: "The covert nature and elusive instrumentalities of unconventional warfare make it difficult for societies under attack to identify the source of the threat and to rally domestic and international opinion."[41] In other words, once conflict was waged through proxies, it was difficult to develop international consensus about the relevant facts, let alone legal violation or justification.

Like proxy conflicts of the Cold War, but to a much larger extent, cyber-conflict is likely to feature ambiguous or disputed facts about what exactly occurred,

including who committed the electronic intrusion or disruption, and on whose behalf they were doing it.[42] Consider again the case of Estonia, in which it took months to compile still murky information about the source of attacks on Estonian computer networks, and many key facts—including ultimate responsibility for directing or encouraging them—remain subject to debate.[43] Evidence of Russian involvement was mostly circumstantial and Russian officials denied involvement.[44] There is also evidence suggesting that the Russian government may have encouraged non-government "patriotic hackers" to conduct attacks, and that other countries, like China, may be relying similarly on legions of quasi-private hackers.[45]

The factual haze that plagued efforts to regulate Cold War proxy conflicts will be significantly exacerbated in the cyber-conflict context because of the greater ability of participants to anonymize or mask their identities and because actions in cyber warfare can be so decentralized and dispersed, and often conducted on private infrastructure.[46] Even if forensic processes can trace a cyber attack to its source, States may be unable to publicize that information in a timely and convincing way, especially when those States are likely to have strong incentive not to discuss the technical details of informational security breaches or reveal their own capabilities to intruders.[47] These are among the reasons that the National Research Council study concluded that "[w]hile in most conflicts, both sides claim that they are acting in self-defense, cyberconflicts are a particularly messy domain in which to air and judge such claims."[48]

Like unconventional conflicts of the Cold War but to an even greater degree, cyber warfare may lack clearly discernable starting and end points or easily visible or verifiable actions and countermoves. This does not mean that drawing legal boundaries is impossible. It does suggest, however, that efforts to promote clear international legal prohibitions, or the accretion of interpretive practice commanding broad consensus, will likely be especially protracted and uncertain.

Power Relations and Regulating Cyber Attacks

The early history of and debates about Article 2(4) also illustrate that competing interpretations of the UN Charter have always reflected allocations of power. Those with more power have greater ability to promote through State practice their preferred interpretation. Moreover, efforts to revise the legal rules may have redistributive effects on power, by affecting the costs and benefits of using certain capabilities.

As described above, a fundamental dispute about Article 2(4) has from the beginning concerned the prohibition's breadth: does Article 2(4) ban military violence only, or does it also ban other forms of coercion, including economic

coercion? Although weak States of the developing world often argued that Article 2(4) prohibited a much broader category of coercion than just military force,[49] that position never took hold. The more restrictive interpretation generally confined to military means and pushed by the United States largely prevailed.

This interpretation suited the United States well during most of the Charter's history. The costs it placed on States of resorting first to conventional armed force in a crisis were high, thereby generally helping to preserve territorial stability and prevent escalation. Meanwhile, the United States could build its defenses beneath the umbrella of nuclear deterrence, grow its economy and expand its influence, all the while relatively free to wield its tremendous economic and diplomatic power without the fear of reciprocal coercion.[50]

Against that historical backdrop, a reason that the United States has an interest in regulating cyber attacks but why it will probably be difficult to do so through international law, whether interpreting existing treaties or custom or negotiating new legal agreements, is because the distribution of emerging cyber-capabilities (offensive and defensive) and vulnerabilities (in terms of ability to block actions as well as ability to withstand or tolerate attacks) may not correspond to the previous or present distribution of power composed of older forms of military and economic might.

Indeed, some US strengths rely on informational interconnectedness and infrastructure that is global, mostly private and rapidly evolving, but these strengths are also therefore inextricably linked to emerging vulnerabilities.[51] Although many experts assess that the United States is currently strong relative to others in terms of some offensive capabilities,[52] several factors make the United States especially vulnerable to cyber attacks, including the extensive interconnectivity of its military and critical infrastructure and its political aversion to heavy regulation of private-sector networks.[53]

Rapidly evolving cyber-capabilities have the potential to alter power balances among States because some are more vulnerable than others, and attacks could have disproportionately large impacts on some countries or their military capabilities.[54] Developing an offensive cyber warfare capability is likely to be less costly than competing economically or militarily with much stronger States.[55] It is therefore not surprising to see some regional rogues or aspirants for power developing offensive cyber warfare capabilities.[56]

As for other major powers, such as Russia and China, they may calculate their strategic interests with respect to cyber warfare and possible legal restrictions on it differently than the United States in light of their own capabilities and vulnerabilities, as well as the degree to which international law constrains their actions.[57] Russia, for example, has proposed to the United Nations a draft statement of principles

that would prohibit the development of cyber attack capabilities, but in the meantime it is investing in the development of such tools.[58] Some analysts are therefore skeptical of Russia's sincerity in proposing such agreements, especially given the difficulties of verification in this arena.[59] China likely sees cyber warfare capabilities as a way of equalizing the conventional military superiority of the United States, and the extent to which public and private lines in China blur may provide China additional advantages in the cyber-conflict realm.[60]

Again, though, consideration of any proposed UN Charter interpretation must account for the processes by which the Charter is interpreted, applied and enforced. The likely factual uncertainty of alleged cyber attacks and the pressures to launch responsive strokes more quickly than those facts can be resolved may require urgent policy decision making amid legal ambiguity. The United States may prefer relatively clear standards with respect to cyber-actions that have immediate destructive effects (at least clear enough to justify military responses or deterrent threats to some scenarios), while at the same time it may prefer some flexibility or permissive vagueness with respect to intelligence collection or some other intrusive measures in cyberspace, so as not to seriously inhibit those activities in which it holds comparative advantages.[61] Other States, however, may see benefits in a different mix of doctrinal line drawing and clarity, in some cases because they are less constrained internally by law than the United States, or because they contemplate using a different mix of cyber-capabilities, or because they see themselves as potential victims (or innocent bystanders) of actions in cyberspace that they would hope to paint legally and diplomatically as impermissible aggression.

In this strategic context, emergent US legal interpretations and declaratory postures may be seen as part of an effort to sustain a legal order that preserves US comparative advantages. In moving toward a view of Article 2(4) that would prohibit some cyber attacks by emphasizing their comparable effects to conventional military attacks, such interpretations help deny that arsenal to others, by raising the costs of its use. At the same time, by casting that prohibition in terms that would in some circumstances help justify resort to military force in self-defense under Article 51, this interpretation lowers the costs to the United States of using or threatening its vast military edge.

That any drawing or redrawing of legal lines creates strategic winners and losers will make it difficult to reach agreement on legal prohibitions, whether through interpretive evolution of the UN Charter or through new legal agreements.[62] Success therefore depends on the ability of proponents not only to articulate but to defend those legal lines using various forms of influence. That is, the strength of a new legal regime to regulate cyber attacks will, as always, depend to a large extent on the allocation of power that cyber-technological developments are reshaping.

Conclusion

As Professor Michael Reisman reminds us,

> [i]nternational law is still largely a decentralized process, in which much lawmaking (particularly for the most innovative matters) is initiated by unilateral claim, whether explicit or behavioral. Claims to change inherited security arrangements . . . ignite a process of counterclaims, responses, replies, and rejoinders until stable expectations of right behavior emerge.[63]

It is possible, but unlikely, that States will soon come together and clarify through new legal instruments the permissible bounds of actions in cyberspace. More likely is a slow accretion of interpretation as crises unfold and claims and counterclaims, reflecting distributions of power in their content and strength, remold the UN Charter regime's contours around new forms of conflict. A policy upshot of this analysis is that, to be effective, legal strategy must be integrated with cyber warfare strategy, including efforts to promote offensive, defensive, preemptive, deterrent and intelligence capabilities amid a security environment that is evolving rapidly and unpredictably.

Notes

1. *See* William J. Lynn III, *Defending a New Domain*, FOREIGN AFFAIRS, Sept.–Oct. 2010, at 97.

2. *Id.* at 98.

3. This definition is based on the one used in the National Research Council's Committee on Offensive Information Warfare's TECHNOLOGY, POLICY, LAW, AND ETHICS REGARDING U.S. ACQUISITION AND USE OF CYBERATTACK CAPABILITIES (William A. Owens, Kenneth W. Dam & Herbert S. Lin eds., 2009) [hereinafter NRC COMMITTEE REPORT].

4. Some of the observations and arguments contained in this article are developed further in Matthew C. Waxman, *Cyber-Attacks as "Force": Back to the Future of Article 2(4)*, YALE JOURNAL OF INTERNATIONAL LAW (forthcoming 2011).

5. *See* Yoram Dinstein, *Computer Network Attacks and Self-Defense*, *in* COMPUTER NETWORK ATTACK AND INTERNATIONAL LAW 99, 114 (Michael N. Schmitt & Brian T. O'Donnell eds., 2002) (Vol. 76, US Naval War College International Law Studies) [hereinafter CNA AND INTERNATIONAL LAW].

6. U.N. Charter art. 2, para. 4.

7. *Id.*, art. 51.

8. *See* THOMAS M. FRANCK, RECOURSE TO FORCE: STATE ACTION AGAINST THREATS AND ARMED ATTACKS 45–52 (2002).

9. For a survey of approaches to these legal questions, see Daniel B. Silver, *Computer Network Attack as a Use of Force under Article 2(4) of the United Nations Charter*, *in* CNA AND INTERNATIONAL LAW, *supra* note 5, at 73. There is continuing debate about whether there is a gap between Articles 2(4) and 51, insofar as a use of force prohibited by 2(4) might not be sufficient

to trigger a right to use military force in self-defense. *See* Albrecht Randelzhofer, *Article 51*, *in* 1 THE CHARTER OF THE UNITED NATIONS: A COMMENTARY 788, 790 (Bruno Simma et al. eds., 2d ed. 2002).

10. *See* Evgeny Morozov, *The Fog of Cyberwar*, NEWSWEEK, Apr. 27, 2009, International Edition, World Affairs, at 0; Jonathan Schwartz, *When Computers Attack*, NEW YORK TIMES, June 24, 2007, § WK, at 1.

11. Press Statement, John Chipman, Director-General of the International Institute for Strategic Studies, The Military Balance 2010 (Feb. 3, 2010), http://www.iiss.org/publications/military-balance/the-military-balance-2010/military-balance-2010-press-statement/.

12. *See* NRC COMMITTEE REPORT, *supra* note 3, at 17–20; Walter Gary Sharp Sr., *The Past, Present, and Future of Cybersecurity*, 4 JOURNAL OF NATIONAL SECURITY LAW & POLICY 13 (2010).

13. The White House, National Security Strategy 27 (2010), *available at* http://www.whitehouse.gov/sites/default/files/rss_viewer/national_security_strategy.pdf.

14. *See* Tom J. Farer, *Political and Economic Coercion in Contemporary International Law*, 79 AMERICAN JOURNAL OF INTERNATIONAL LAW 405, 408 (1985); NRC COMMITTEE REPORT, *supra* note 3, at 253.

15. *See* YORAM DINSTEIN, WAR, AGGRESSION AND SELF-DEFENCE 18 (2d ed. 1994); Hans Kelsen, *General International Law and the Law of the United Nations*, *in* THE UNITED NATIONS: TEN YEARS' LEGAL PROGRESS 1, 5 (Gesina H.J. Van Der Molen et al. eds., 1956); AHMED M. RIFAAT, INTERNATIONAL AGGRESSION: A STUDY OF THE LEGAL CONCEPT 120, 234 (1980); Albrecht Randelzhofer, *Article 2(4)*, *in* 1 THE CHARTER OF THE UNITED NATIONS: A COMMENTARY, *supra* note 9, at 118.

16. *See* JULIUS STONE, CONFLICT THROUGH CONSENSUS 87–104 (1977).

17. *See* Farer, *supra* note 14, at 406.

18. Declaration on the Inadmissibility of Intervention into the Domestic Affairs of States and the Protection of Their Independence and Sovereignty, U.N. GAOR, 20th Sess., Supp. No. 14, at 11, U.N. Doc. A/6014 (Dec. 21, 1965) ("all . . . forms of interference or attempted threats against the personality of the State or against its political, economic and cultural elements, are condemned" and "No State may use or encourage the use of economic, political or any other type of measures to coerce another State in order to obtain from it the subordination of the exercise of its sovereign rights or to secure from it advantages of any kind.").

19. *See* NRC COMMITTEE REPORT, *supra* note 3, at 33–34; *see also* IAN BROWNLIE, INTERNATIONAL LAW AND THE USE OF FORCE BY STATES 362–63 (1963) (defining "use of force" by looking beyond immediate death or injury from impact to the destructive effects).

20. *See* Michael N. Schmitt, *Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework*, 37 COLUMBIA JOURNAL OF TRANSNATIONAL LAW 885, 914–15 (1999).

21. *See, e.g.*, Silver, *supra* note 9, at 92.

22. *See, e.g.*, RICHARD A. CLARKE, CYBER WAR 178 (2010) (proposing a doctrine of *cyber equivalency*) (italics in original).

23. *Reprinted in* CNA AND INTERNATIONAL LAW, *supra* note 5, at 459, 483.

24. *See id.*

25. Secretary of State Hillary Rodham Clinton, Remarks on Internet Freedom at the Newseum, Washington, D.C. (Jan. 21, 2010), http://www.state.gov/secretary/rm/2010/01/135519.htm.

26. Responses by Lieutenant General Keith Alexander, Nominee for Commander, United States Cyber Command to Senate Armed Services Committee Advance Questions (Apr. 15, 2010), at 11, http://armed-services.senate.gov/statemnt/2010/04%20April/Alexander%2004-15-10.pdf.

27. *Id.* at 12.

28. *See* NRC COMMITTEE REPORT, *supra* note 3, at 259–61.

29. Thomas M. Franck, *Who Killed Article 2(4)? Or: Changing Norms Governing the Use of Force by States*, 64 AMERICAN JOURNAL OF INTERNATIONAL LAW 809, 812 (1970).

30. *Quoted in* Kim Zetter, *Former NSA Director: Countries Spewing Cyber Attacks Should Be Held Responsible*, WIRED.COM (July 29, 2010), http://www.wired.com/threatlevel/2010/07/hayden-at-blackhat/.

31. *See* Franck, *supra* note 29, at 812–20.

32. Alberto R. Coll, *Unconventional Warfare, Liberal Democracies, and International Order*, *in* LEGAL AND MORAL CONSTRAINTS ON LOW-INTENSITY CONFLICT 3, 3 (Alberto R. Coll, James S. Ord & Stephen A. Rose eds., 1995) (Vol. 67, US Naval War College International Law Studies).

33. Robert F. Turner, *State Sovereignty, International Law, and the Use of Force in Countering Low-Intensity Aggression in the Modern World*, *in id.* at 43, 60.

34. *See* Oscar Schachter, *The Right of States to Use Armed Force*, 82 MICHIGAN LAW REVIEW 1620, 1645–46 (1984).

35. *See* NRC COMMITTEE REPORT, *supra* note 3, at 138–41, 252; Duncan B. Hollis, *Why States Need an International Law for Information Operations*, 11 LEWIS & CLARK LAW REVIEW 1023, 1031–32 (2007); John Markoff et al., *In Digital Combat, U.S. Finds No Easy Deterrent*, NEW YORK TIMES, Jan. 26, 2010, at 1 (discussing difficulties of determining source of cyber attacks).

36. *See* Jack Goldsmith, *The New Vulnerability*, NEW REPUBLIC, June 24, 2010, at 21, 23.

37. Lynn, *supra* note 1, at 99.

38. FRANCK, *supra* note 8, at 820.

39. *Id.*

40. *See* Coll, *supra* note 32, at 15–16.

41. *See id.* at 4.

42. *See* Hollis, *supra* note 35, at 1031–32.

43. *See* NRC COMMITTEE REPORT, *supra* note 3, at 173.

44. *See id.*

45. *See* Anne Applebaum, *For Estonia and NATO, a New Kind of War*, WASHINGTON POST, May 22, 2007, at A15; David E. Sanger et al., *U.S. Plans Attack and Defense in Web Warfare*, NEW YORK TIMES, Apr. 28, 2009, at A1.

46. *See* Sean P. Kanuck, *Information Warfare: New Challenges for Public International Law*, 37 HARVARD INTERNATIONAL LAW JOURNAL 272, 286–88 (1996).

47. The disclosures by Deputy Secretary Lynn described earlier are a case in point, as it took several years for the government to declassify the information, and that decision itself was controversial. *See* Ellen Nakashima, *Defense Official Discloses Cyberattack*, WASHINGTON POST, Aug. 24, 2010, at A3.

48. *See* NRC COMMITTEE REPORT, *supra* note 3, at 315.

49. *See* STONE, *supra* note 16, at 96; Julius Stone, *Hopes and Loopholes in the 1974 Definition of Aggression*, 71 AMERICAN JOURNAL OF INTERNATIONAL LAW 224 (1977).

50. *See* Tom J. Farer & Christopher C. Joyner, *The United States and the Use of Force*, 1 TRANSNATIONAL LAW & CONTEMPORARY PROBLEMS 15, 22–23 (1991).

51. *See* PHILIP BOBBITT, THE SHIELD OF ACHILLES 792–94 (2002).

52. *See* Jack Goldsmith, *Can We Stop the Global Cyber Arms Race?*, WASHINGTON POST, Feb. 1, 2010, at A17 ("the U.S. government has perhaps the world's most powerful and sophisticated offensive cyberattack capability").

53. *See* CLARKE, *supra* note 22, at 226–27.

54. *See id.* at 259. For views more skeptical that cyber-capabilities will radically alter power balances, see generally MARTIN C. LIBICKI, CONQUEST IN CYBERSPACE (2007); GREGORY J. RATTRAY, STRATEGIC WARFARE IN CYBERSPACE (2001).

55. *See* STEWART BAKER, SKATING ON STILTS 218–20 (2010).

56. *See* Choe Sang-Hun & John Markoff, *Cyberattacks Jam Government and Commercial Web Sites in U.S. and South Korea*, NEW YORK TIMES, July 9, 2009, at A4 (North Korea).

57. For discussion of such legal jockeying among States, see Sean Kanuck, *Sovereign Discourse on Cyber Conflict Under International Law*, 88 TEXAS LAW REVIEW 1571, 1585–87 (2010).

58. *See* NRC COMMITTEE REPORT, *supra* note 3, at 329–32; John Markoff & Andrew E. Kramer, *U.S. and Russia Differ on Treaty for Cyberspace*, NEW YORK TIMES, June 28, 2009, at A1.

59. *See* BAKER, *supra* note 55, at 230–31.

60. *See* NRC COMMITTEE REPORT, *supra* note 3, at 332–33; Office of the Secretary of Defense, Annual Report to Congress: Military Power of the People's Republic of China 27–28 (2009).

61. As a general matter, international law has very little to say about intelligence collection. *See* Kanuck, *supra* note 46, at 275–76.

62. *See* Goldsmith, *supra* note 36, at 26.

63. W. Michael Reisman, *Assessing Claims to Revise the Laws of War*, 97 AMERICAN JOURNAL OF INTERNATIONAL LAW 82, 82 (2003).